PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-297820
(43)Date of publication of application : 10.11.1995

(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

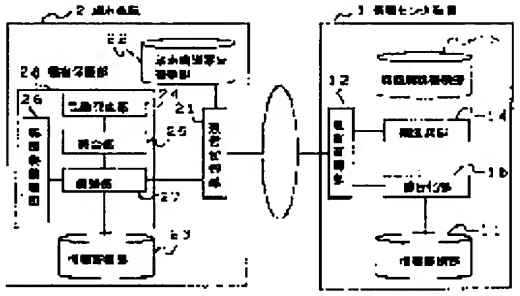
(21)Application number : 06-091023
(22)Date of filing : 28.04.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
TOSHIBA CORP

(72)Inventor : YAMANAKA KIYOSHI
KOYAIZU IKURO
KANDA MASASUKI
MATSUDA NOBUHIRO
SEKIYA KUNIHIKO
YAHATA MEIKI

(54) METHOD AND SYSTEM FOR DIGITAL INFORMATION PROTECTION

(57)Abstract:
PURPOSE: To provide a method and a system for digital information protection system which prevent the illegal use of information without disturbing the privacy.
CONSTITUTION: When information is received from an information center device 1 to a terminal equipment 2, enciphered information is received and is stored in an information storage part 23; and when information is used, random numbers generated by a random number generation part 24 are transmitted from the terminal equipment 2 to the information center device 1 to request a deciphering key for deciphering information, and random numbers and the deciphering key are enciphered by a terminal secret key and are transmitted from the information center device 1 to the terminal equipment 2. The terminal equipment 2 deciphers random numbers and the deciphering key and collates transmitted random numbers and received those with each other; and when they coincide with each other as the result of collation, the terminal equipment 2 deciphers digital information and erases random numbers and the deciphering key.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－297820

(43)公開日　平成７年(1995)11月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｇ０９Ｃ	1/00		9364－5Ｌ			
				Ｈ０４Ｌ	9/ 02	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平6－91023

(22)出願日　平成６年(1994)４月28日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　小柳津　育郎
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　吉田　精孝

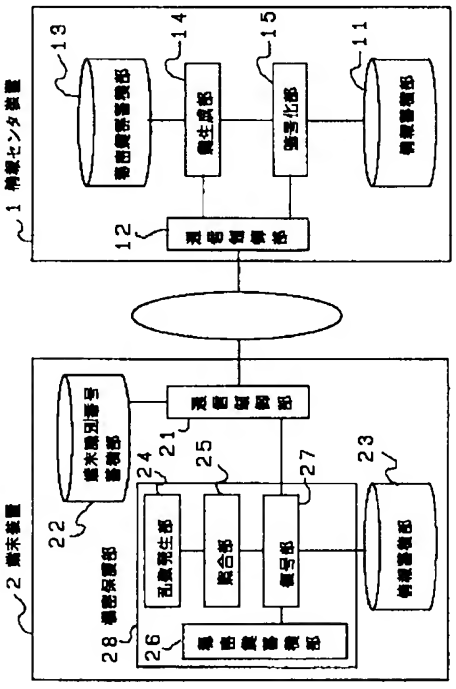
最終頁に続く

(54)【発明の名称】　ディジタル情報保護システム及びその方法

(57)【要約】

【目的】　プライバシを侵害すること無く情報の不正使用を防止できるディジタル情報保護システム及びその方法を提供する。

【構成】　情報センタ装置１から端末装置２に情報を受信する際には暗号化された情報受信して情報蓄積部２３に蓄積しておき、情報を使用する際に端末装置２から情報センタ装置１に乱数発生部２４によって発生した乱数を送信して情報を復号する復号用鍵を要求し、情報センタ装置１から乱数と復号鍵を端末秘密鍵によって暗号化して端末装置２に送信する。端末装置２では乱数と復号鍵を復号して送信した乱数と受信した乱数を照合し、照合の結果これらが一致したときにディジタル情報の復号を行い、乱数と復号用鍵を消去する。



1

【特許請求の範囲】

【請求項１】　共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるディジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するディジタル情報保護システムであって、

前記情報センタ装置は、ディジタル情報を蓄積する情報蓄積手段と、

端末装置との通信を行なう通信制御手段と、

複数の端末装置を一意に特定する端末識別番号と端末秘密鍵とを対応させて格納する秘密鍵群蓄積手段と、

情報の暗号化用鍵及び復号用鍵を生成する鍵生成手段と、

前記暗号化用鍵を用いてディジタル情報を暗号化する暗号化手段と、

前記端末装置から要求のあったディジタル情報を前記暗号化手段により暗号化して前記端末装置に送信する情報送信手段と、

前記端末装置から復号用鍵の要求があったときに、該端末装置から受信した乱数及び前記復号用鍵を該端末装置に対応する前記端末秘密鍵を用いて暗号化して前記端末装置に送信する復号鍵送信手段とを備え、

前記端末装置は、前記情報センタ装置との通信を行なう通信制御手段と、

前記端末識別番号を格納する端末識別番号蓄積手段と、

ディジタル情報を蓄積する情報蓄積手段と、

乱数データを発生する乱数発生手段と、

前記情報センタ装置に対して前記復号鍵を要求する際に前記乱数データを前記情報センタ装置に送信する復号鍵要求手段と、

前記発生した乱数データと前記情報センタ装置から受信した乱数データの値を照合する照合手段と、

端末装置の秘密鍵を格納する秘密鍵蓄積手段と、

前記照合手段の照合結果に基づいて、前記秘密鍵を用いて前記復号用鍵及びディジタル情報を復号する復号手段と、

少なくとも前記乱数発生手段、照合手段、秘密鍵蓄積手段、復号手段を秘密保護する保護手段を備えることを特徴とするディジタル情報保護システム。

【請求項２】　共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるディジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するディジタル情報保護方法であって、

情報要求の際に前記端末装置では、所望のディジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信し、

前記情報識別番号を受信した情報センタ装置では、前記

2

受信した情報識別番号に対応したディジタル情報を情報蓄積手段より取り出し、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記ディジタル情報を暗号化して前記端末装置に送信し、

該暗号化ディジタル情報を受信した端末装置では、受信した暗号化ディジタル情報を情報識別番号と共に情報蓄積手段に蓄積し、

該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号を前記情報蓄積手段より取り出し、該情報識別番号を、乱数発生手段で発生した乱数及び端末識別番号と共に前記情報センタ装置に送信し、

前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵を生成すると共に、該端末識別番号に相当する端末秘密鍵により、前記復号鍵と乱数の結合ビット列を暗号化して前記端末装置に送信し、

この後、端末装置では、前記情報センタ装置からの受信情報を予め蓄積されている端末秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とを比較し、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化ディジタル情報を復号することを特徴とするディジタル情報保護方法。

【請求項３】　前記情報識別番号に加え、端末装置または情報センタ装置で生成した１つ以上のパラメータを組合わせた秘密関数で計算した暗号鍵及び復号鍵により、ディジタル情報の暗号化及び復号を行うことを特徴とする請求項２に記載のディジタル情報保護方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、音楽、映像、プログラム等の暗号化されたディジタル著作物情報を、電気通信網または有線放送網などの公衆網ないし専用網を介して受信して蓄積した後、情報を利用する際に、復号鍵を配送するディジタル情報保護システム及びその方法に関するものである。

【０００２】

【従来の技術】近年、音声・動画・静止画等のディジタル情報圧縮技術（例えば、ＭＰＥＧ＝Moving Picture Image Expert Group，ＪＰＥＧ=Joint Photographic Expert Group　など）、及びＩＳＤＮを代表とする高速ディジタル通信技術の発達により、音楽・映像・絵画・書籍等の著作物をディジタル情報に変換、圧縮符号化して通信回線を利用して送信することが実現可能となってきた。

【０００３】映像等のディジタル情報に比べデータ量の少ないコンピュータソフトウェアでは、既に、パソコン

通信等を利用した配送サービスを実施している例がある。また、米国内において最近サービスが開始されたＣＤ－ＲＯＭによるコンピュータソフト販売の方法は、暗号化された販売用ソフト及び暗号化されていないデモ用ソフトを格納するＣＤ－ＲＯＭを低価格で販売・配布し、利用者はデモ用ソフトで試用後、購入希望後をサービスセンターに電話で申し込んで復号鍵を受け取る形式をとっている。

【０００４】

【発明が解決しようとする課題】従来のパソコン通信などによる、コンピュータソフト販売の場合、ソフトウエアの暗号化がなされておらず、従来のフロッピーディスクなどのパッケージによるソフトウェア販売方法に比べ違法コピーをより容易にさせる環境を提供することになる。また、ＣＤ－ＲＯＭによる配布の場合は、電話にて復号鍵をセンタより受け取る際に、センタオペレータを介在するため、人手がかかり、かつプライバシ侵害の問題が生じる。

【０００５】本発明の目的は上記の問題点に鑑み、端末の記録状況がセンタで把握でき、不正コピーを防止するディジタル情報保護システム及びその方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項１では、共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるディジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するディジタル情報保護システムであって、前記情報センタ装置は、ディジタル情報を蓄積する情報蓄積手段と、端末装置との通信を行なう通信制御手段と、複数の端末装置を一意に特定する端末識別番号と端末秘密鍵とを対応させて格納する秘密鍵群蓄積手段と、情報の暗号化用鍵及び復号用鍵を生成する鍵生成手段と、前記暗号化用鍵を用いてディジタル情報を暗号化する暗号化手段と、前記端末装置から要求のあったディジタル情報を前記暗号化手段により暗号化して前記端末装置に送信する情報送信手段と、前記端末装置から復号用鍵の要求があったときに、該端末装置から受信した乱数及び前記復号用鍵を該端末装置に対応する前記端末秘密鍵を用いて暗号化して前記端末装置に送信する復号鍵送信手段とを備え、前記端末装置は、前記情報センタ装置との通信を行なう通信制御手段と、前記端末識別番号を格納する端末識別番号蓄積手段と、ディジタル情報を蓄積する情報蓄積手段と、乱数データを発生する乱数発生手段と、前記情報センタ装置に対して前記復号鍵を要求する際に前記乱数データを前記情報センタ装置に送信する復号鍵要求手段と、前記発生した乱数データと前記情報センタ装置から受信した乱数データの値を照合する照合手段と、端末装置の秘密鍵を格納する秘密鍵蓄積手段と、前記照合手段の照合結果に基づいて、前記秘密鍵を用いて前記復号用鍵及びディジタル情報を復号する復号手段と、少なくとも前記乱数発生手段、照合手段、秘密鍵蓄積手段、復号手段を秘密保護する保護手段を備えるディジタル情報保護システムを提案する。

【０００７】また、請求項２では、共通鍵暗号方式により暗号化された音声、音楽、映像、文字の少なくとも一つからなるディジタル情報を情報センタ装置から通信回線を経由して受信し端末装置に蓄積して利用の都度、前記端末装置から情報センタ装置に復号鍵を要求するディジタル情報保護方法であって、情報要求の際に前記端末装置では、所望のディジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信し、前記情報識別番号を受信した情報センタ装置では、前記受信した情報識別番号に対応したディジタル情報を情報蓄積手段より取り出し、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記ディジタル情報を暗号化して前記端末装置に送信し、該暗号化ディジタル情報を受信した端末装置では、受信した暗号化ディジタル情報を情報識別番号と共に情報蓄積手段に蓄積し、該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号を前記情報蓄積手段より取り出し、該情報識別番号を、乱数発生手段で発生した乱数及び端末識別番号と共に前記情報センタ装置に送信し、前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵を生成すると共に、該端末識別番号に相当する端末秘密鍵により、前記復号鍵と乱数の結合ビット列を暗号化して前記端末装置に送信し、この後、端末装置では、前記情報センタ装置からの受信情報を予め蓄積されている端末秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とを比較し、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化ディジタル情報を復号するディジタル情報保護方法を提案する。

【０００８】また、請求項３では、請求項２記載のディジタル情報保護方法において、前記情報識別番号に加え、端末装置または情報センタ装置で生成した１つ以上のパラメータを組合わせた秘密関数で計算した暗号鍵及び復号鍵により、ディジタル情報の暗号化及び復号を行うディジタル情報保護方法を提案する。

【０００９】上記課題を解決するため、共通鍵暗号方式により暗号化されたディジタル情報本体を通信回線利用により配送した後、情報を利用する際に、１回のみ復号可能な復号鍵を通信回線により配送するシステム及び方法に関する。

【００１０】

【作用】本発明の請求項１によれば、端末装置から情報

センタに情報を要求する際には、端末装置は、通信制御手段によって情報センタ装置に接続して、必要なディジタル情報を検索し、情報本体の配送要求を行なう。これにより、情報本体の配送要求を受けた情報センタ装置では、要求されたディジタル情報が情報蓄積手段から取り出されると共に、鍵生成手段によって暗号鍵が生成され、暗号化手段により前記取り出されたディジタル情報が該暗号鍵により暗号化されて前記端末装置に送信される。この後、端末装置では、受信した暗号化ディジタル情報が情報蓄積手段に蓄積される。該蓄積されたディジタル情報を利用する際には、端末装置では、情報蓄積手段内の情報から利用したい情報が選択され、乱数発生手段により乱数が生成された後、復号鍵要求手段により該乱数が情報センタ装置に送信される。該乱数を受信した情報センタ装置では、鍵生成手段により復号鍵が生成され、復号鍵送信手段によって、端末装置の秘密鍵を用いて、例えば前記復号鍵を乱数のビット単位に連結した結合ビット列が暗号化されて端末装置に送信される。端末装置では、前記情報センタ装置からの受信情報を復号手段で秘密鍵蓄積手段より取り出した端末装置の秘密鍵で復号して、乱数と復号鍵を取り出し、該乱数と送信前に端末装置で生成した乱数とが照合手段によって照合され、この照合の結果、乱数が一致しない場合には、情報の復号が禁止される。また、一致した場合には、復号手段によって該復号鍵を用いて情報蓄積手段内の暗号化ディジタル情報が復号された後、前記乱数及び復号鍵が消去される。また、端末装置での、乱数発生手段、照合手段、復号手段及び秘密鍵蓄積手段はすべて保護手段によって封印等されて端末装置の利用者から隔離され、機密保護されている。

【００１１】また、請求項２によれば、端末装置から情報センタに対して情報を要求する際には、前記端末装置によって所望のディジタル情報を一意に特定する情報識別番号を前記情報センタ装置に送信され、前記情報識別番号を受信した情報センタ装置により、前記受信した情報識別番号に対応したディジタル情報が情報蓄積手段より取り出され、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した暗号鍵を用いて前記ディジタル情報が暗号化されて前記端末装置に送信される。この後、前記暗号化ディジタル情報を受信した端末装置では、受信した暗号化ディジタル情報が情報識別番号と共に情報蓄積手段に蓄積され、該情報蓄積手段に蓄積された情報を利用するときに、利用したい情報の情報識別番号が前記情報蓄積手段より取り出され、該情報識別番号が、乱数発生手段で発生された乱数及び端末識別番号と共に前記情報センタ装置に送信される。前記情報識別番号、乱数及び端末識別番号を受信した情報センタ装置では、鍵生成手段により前記情報識別番号をパラメータとする秘密関数で計算した復号鍵が生成されると共に、該端末識別番号に相当する端末秘密鍵により、前記復号鍵と乱数の結合ビット列が暗号化されて前記端末装置に送信される。この後、端末装置では、前記情報センタ装置からの受信情報が端末秘密鍵を用いて復号されて、乱数と復号鍵が取り出され、該乱数と送信前に端末装置で生成した乱数とが比較され、該乱数が一致した場合のみ、該復号鍵により端末装置の情報蓄積手段内の暗号化ディジタル情報が復号される。

【００１２】また、請求項３によれば、前記情報識別番号に加え、端末装置または情報センタ装置で生成された１つ以上のパラメータを組合わせた秘密関数を用いて計算された暗号鍵及び復号鍵により、ディジタル情報の暗号化及び復号が行われる。

【００１３】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図１は、本発明の第１の実施例のディジタル情報保護システムを示す構成図である。図において、１は情報センタ装置で、ディジタル情報を蓄積する情報蓄積部１１、後述する端末装置２との通信を行なう通信制御部１２、複数の端末装置を一意に特定する端末識別番号と秘密鍵の対応を格納する秘密鍵群蓄積部１３、共通鍵暗号方式による情報の暗号化および、復号を行なう鍵を生成する鍵生成部１４、ディジタル情報を暗号化する暗号化部１５を備えている。

【００１４】２は端末装置で、情報センタ装置１との通信を行なう通信制御部２１、端末識別番号を格納する端末識別番号蓄積部２２、ディジタル情報を蓄積する情報蓄積部２３、乱数データを発生する乱数発生部２４、乱数データを照合する照合部２５、端末装置の秘密鍵を格納する秘密鍵蓄積部２６、鍵情報及びディジタル情報を復号する復号部２７、前記乱数発生部２４、照合部２５、秘密鍵蓄積部２６、及び復号部２７を少なくとも機密保護する機密保護部２８である。

【００１５】ここで、機密保護部２８による機密保護の方法としては、「この部分はユーザが開封することを禁止する」などの注意書きを明記した簡易な封印、カスタムＬＳＩにより物理的に外部から侵害できない専用ハードによる保護（例:R.Mori and M.Kawahara'Supredistribution:The Concept and the Architecture'Trans.IEICE,E-73-No.7,1990.7）など様々な方法が提案されており、これらのいずれを用いることも可能である。

【００１６】次に、前述の構成よりなる第１の実施例において、情報センタ装置１から端末装置２にディジタル情報を受信して端末装置２に蓄積するまでの情報受信・蓄積過程の動作手順を図２に示すフローチャートに基づいて説明する。なお、端末装置２と情報センタ装置１間の回線はＩＳＤＮなどの公衆通信回線を利用する例で説明する。

【００１７】端末装置２は、情報センタ装置１に接続して（ＳＡ１）、必要なディジタル情報を検索し、該情報を一意に特定する情報識別番号を情報センタ装置１に送

信して情報本体の配送要求を行なう（ＳＡ２）。ここで、情報識別番号は、例えば音楽情報の場合、国際レコーディングコード（ＩＳＲＣ）など、全世界共通コードまたは、該情報提供業者が独自に付与した情報を一意に特定できる番号等である。

【００１８】情報本体の配送要求を受けた情報センタ装置１は、情報識別番号に対応したディジタル情報を情報蓄積部１１より取り出し（ＳＡ３）、鍵生成部１４によって前記情報識別番号をパラメータとする秘密関数により暗号鍵Ｋｓを生成し（ＳＡ４）、暗号化部１５で前記取り出されたディジタル情報を該暗号鍵により暗号化して（ＳＡ５）、端末装置２に送信する（ＳＡ６）。

【００１９】ここで、暗号化アルゴリズムとして、例えばＦＥＡＬ，ＤＥＳなどの共通鍵暗号方式を使用することができる。また、秘密関数は、情報センタ装置１のみが知っており、端末装置２または端末利用者が入力パラメータから容易に結果を推定できない一方向性関数などである。

【００２０】この後、端末装置２では、図３に示すように、受信した暗号化ディジタル情報を情報識別番号とともに情報蓄積部２３に蓄積する（ＳＡ７）。

【００２１】次に、第１の実施例においてディジタル情報を利用する情報利用過程の動作手順を図４に示すフローチャートに基づいて説明する。端末装置２では、情報蓄積部２３に受信・蓄積したディジタル情報から利用したい情報を選択し、該情報の情報識別番号を取り出す（ＳＢ１）。次いで、乱数発生部２４で乱数Ｒを生成した後（ＳＢ２）、通信制御部２１を介して情報センタ装置１に接続し（ＳＢ３）、前記情報に対応する情報識別番号、乱数Ｒおよび、端末識別番号蓄積部２２より取り出した端末識別番号とともに情報センタ装置１に送信する（ＳＢ４）。

【００２２】これらの情報受信した情報センタ装置１では、鍵生成部１４により前記受信した情報識別番号をパラメータとする秘密関数で計算した復号鍵Ｋｓを生成する（ＳＢ５）。ここで、秘密関数は前記暗号鍵を生成する際に適用した同一の秘密関数である。

【００２３】次に、情報センタ装置１は、暗号化部１５で、秘密鍵群蓄積部１３より取り出した該端末識別番号に対応する端末秘密鍵Ｋｉにより、前記復号鍵Ｋｓと乱数Ｒをビット単位に連結した結合ビット列Ｋｓ‖Ｒを暗号化し（ＳＢ６）、端末装置２に送信する（ＳＢ７）。図５に、情報センタ装置１の秘密鍵群蓄積部１３の情報内容を示す。秘密鍵群蓄積部１３には端末識別番号（ＩＤ１，ＩＤ２，…）と端末秘密鍵（Ｋ１，Ｋ２，…）が対になって蓄積されている。

【００２４】端末装置２では、前記情報センタ装置１からの受信情報を復号部２７で秘密鍵蓄積部２６より取り出した端末の秘密鍵Ｋｉで復号して（ＳＢ８）、乱数Ｒと復号鍵Ｋｓを取り出し、該乱数Ｒと送信前に端末装置２で生成した乱数とを比較する（ＳＢ９）。この比較の結果、乱数が一致しない場合には、情報の復号を禁止する（ＳＢ１０）。また、一致した場合には、復号部２７で該復号鍵Ｋｓにより情報蓄積部２３内の暗号化ディジタル情報を復号した後（ＳＢ１１）、前記乱数及び復号鍵を消去する（ＳＢ１２）。なお、端末装置２での、乱数発生、乱数照合、復号処理及び秘密鍵蓄積部はすべて機密保護部２８内に封印されて端末装置２の利用者から隔離されている。

【００２５】本第１の実施例によれば、情報を利用する際、情報センタ装置から復号鍵を受信して１回だけ復号できるしくみが提供可能である。しかも、乱数を端末装置２で生成して情報センタ装置１に送信した後、情報センタ装置１では復号鍵と乱数に暗号化して端末装置２に返送することにより、端末装置２と情報センタ装置１との間の送受信情報を盗聴して、同一のトランザクションを生成する疑似センタをパソコン等で構成して同一のディジタル情報をセンタ課金なしに不正利用することを不可能としている。さらに、従来のＣＤ－ＲＯＭによる情報の配布等に比べて個人のプライバシを侵害することもない。

【００２６】次に、情報センタ装置１からディジタル情報を受信して端末装置２に蓄積するまでの情報受信・蓄積過程の動作手順の第２の実施例を図６に示すフローチャートに基づいて説明する。ここで、第２の実施例における装置構成は、図１に示す第１の実施例の構成と同様である。また、図２、図３、図４に示した第１の実施例では、各情報識別番号に対して暗号化・復号鍵が一意に定まるのに対して、第２の実施例では、同一情報識別番号であっても異なる暗号化・復号鍵を生成できるように情報識別番号に加え、端末装置２または情報センタ装置１で生成した１つまたは複数のパラメータを組合せた秘密関数で暗号化・復号鍵を計算しており、これにより端末装置２内の情報蓄積部２３に蓄積されているディジタル情報の暗号攻撃（暗号解読処理）に対して安全性をより強固にしている。

【００２７】図６に示す第２の実施例では、鍵の生成パラメータとして、情報識別番号、端末識別番号及び、送信年月日の３つのパラメータを利用した場合の例で説明する。

【００２８】端末装置２は、情報センタ装置１に接続して（ＳＣ１）、必要なディジタル情報を検索し、端末識別番号蓄積部２２より取り出した端末識別番号と該情報を一意に特定する情報識別番号を情報センタ装置１に送信して情報本体の配送要求を行なう（ＳＣ２）。

【００２９】情報センタ装置１では、前記受信した情報識別番号に対応したディジタル情報を情報蓄積部１１より取り出す（ＳＣ３）。次いで、鍵生成部１４で前記情報識別番号、端末識別番号及び、作成年月日を組合せたパラメータとする秘密関数により暗号鍵を生成する（Ｓ

Ｃ４）。鍵生成用情報としては、受信年月日、端末識別番号以外に情報センタ装置１で生成する乱数、作成時刻など様々なものが考えられ、これらを用いることも可能である。

【００３０】この後、情報センタ装置１は、暗号化部１５で前記取り出されたディジタル情報を該暗号鍵により暗号化して（ＳＣ５）、情報識別番号、端末識別番号以外の鍵生成用情報（本実施例の場合、作成年月日）と共に端末装置２に送信する（ＳＣ６）。

【００３１】これらを受信した端末装置２では、図７に示すように受信した暗号化ディジタル情報を情報識別番号、鍵生成用情報（作成年月日）と共に情報蓄積部２３に蓄積する（ＳＣ７）。

【００３２】次に、第２の実施例においてディジタル情報を利用する情報利用過程の動作手順を図８に示すフローチャートに基づいて説明する。

【００３３】端末装置２では、情報蓄積部２３に受信・蓄積したディジタル情報から利用したい情報を選択し、該情報の情報識別番号および、鍵生成用情報を取り出す（ＳＤ１）。次いで、乱数発生部２４で乱数Ｒを生成した後（ＳＤ２）、情報センタ装置１に接続して（ＳＤ３）、前記情報に対応する情報識別番号、乱数Ｒ、端末識別番号蓄積部２２より取り出した端末識別番号および、鍵生成用情報と共に情報センタ装置１に送信する（ＳＤ４）。

【００３４】情報センタ装置１では、鍵生成部１４で前記受信した情報識別番号、端末識別番号、及び鍵生成用情報のうち前記情報を暗号化した時と同じパラメータを利用して秘密関数により計算した復号鍵Ｋｓを生成する（ＳＤ５）。この後、暗号化部１５で、秘密鍵群蓄積部１３より取り出した該端末識別番号ＩＤｉに対応する端末秘密鍵Ｋｉにより、前記復号鍵Ｋｓと乱数Ｒの結合ビット列Ｋｓ‖Ｒを暗号化し（ＳＤ６）、端末装置２に送信する（ＳＤ７）。

【００３５】端末装置２では、前記情報センタ装置１からの受信情報を復号部２７で秘密鍵蓄積部２６より取り出した端末の秘密鍵Ｋｉで復号して（ＳＤ８）、乱数Ｒと復号鍵Ｋｓを取り出し、該乱数Ｒと送信前に端末装置２で生成した乱数を比較する（ＳＤ９）。この比較の結果、乱数が一致しない場合には、情報の復号を禁止する（ＳＤ１０）。また、一致した場合には、復号部２７で該復号鍵Ｋｓにより情報蓄積部２３内の該暗号化ディジタル情報を復号した後（ＳＤ１１）、前記乱数及び復号鍵を消去する（ＳＤ１２）。

【００３６】なお、以上の第１及び第２の実施例はいずれも、ＩＳＤＮなどの公衆通信回線を利用する場合の例で示したが、専用線などコネクションレスの回線にも適用できる。その場合は、図２、図４、図６、図８のそれぞれで「情報センタ装置と回線接続」の動作は不要である。

【００３７】また、以上の実施例は、端末装置２が情報センタ装置１にディジタル情報を指定して情報の送信を依頼する例で示したが、情報センタ装置１で選択したディジタル情報を端末装置２で受信するシステムにも適用可能である。

【００３８】さらに、本発明は、コンピュータソフトウェアのみならず、全てに暗号化ディジタル情報の通信利用による配送の際に適用できることはいうまでもない。

【００３９】

【発明の効果】以上説明したように本発明の請求項１記載のディジタル情報保護システムによれば、暗号化されたディジタル情報本体を通信回線利用により配送した後、情報を利用する際に、１回のみ利用可能な復号鍵を通信回線により配送すると共に、端末装置において乱数を生成して情報センタ装置に送信して、情報センタ装置では復号鍵と乱数を暗号化して端末装置に返送しているので、端末装置と情報センタ装置間の送受信情報を盗聴して同一のトランザクションを生成する疑似センタにより同一ディジタル情報の課金なしの不正利用を防止することができる。さらに、個人のプライバシを侵害することもない。

【００４０】また、請求項２記載のディジタル情報保護方法によれば、暗号化されたディジタル情報本体を通信回線利用により配送した後、情報を利用する際に、１回のみ利用可能な復号鍵を通信回線により配送すると共に、端末装置において乱数を生成して情報センタ装置に送信して、情報センタ装置では復号鍵と乱数を暗号化して端末装置に返送しているので、端末装置と情報センタ装置間の送受信情報を盗聴して同一のトランザクションを生成する疑似センタにより同一ディジタル情報の課金なしの不正利用を防止することができると共に、個人のプライバシを侵害することもない。

【００４１】さらに、請求項３によれば、上記の効果に加えて、情報識別番号だけでなく端末識別番号、作成年月日等のパラメータを組み合わせて暗号鍵を生成しているため、各同一のディジタル情報に対して常に異なる復号鍵を生成することができるので、安全性の高い鍵配送システムが可能となる大きな利点がある。また、情報センタ装置に複数の端末装置に対して各ディジタル情報ごとの暗号鍵を蓄積しておく必要がないため、安全性と情報センタ装置の資源の有効利用を図ることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例のディジタル情報保護システムを示す構成図

【図２】本発明の第１の実施例におけるディジタル情報の受信・蓄積動作手順を示すフローチャート

【図３】第１の実施例における端末装置の情報蓄積部内の情報内容を示す図

【図４】第１の実施例におけるディジタル情報を利用する際の動作手順を示すフローチャート

11

【図５】第１の実施例における情報センタ装置の秘密鍵群蓄積部の情報内容を示す図

【図６】本発明の第２の実施例におけるディジタル情報の受信・蓄積動作手順を示すフローチャート

【図７】第２の実施例における端末装置の情報蓄積部内の情報内容を示す図

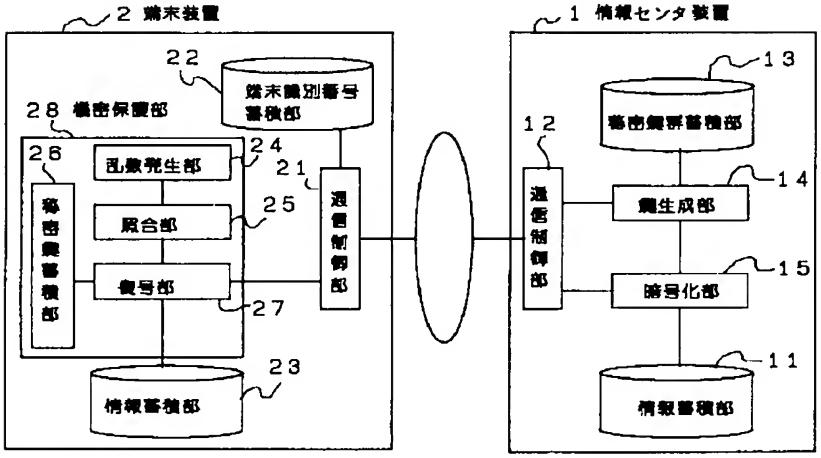
【図８】第２の実施例におけるディジタル情報を利用する際の動作手順を示すフローチャート　＊

12

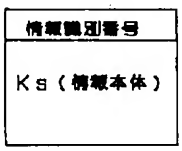
＊【符号の説明】

１…情報センタ装置、２…端末装置、１１…情報蓄積部、１２…通信制御部、１３…秘密鍵群蓄積部、１４…鍵生成部、１５…暗号化部、２１…通信制御部、２２…端末識別番号蓄積部、２３…情報蓄積部、２４…乱数発生部、２５…照合部、２６…秘密鍵蓄積部、２７…復号部、２８…機密保護部。

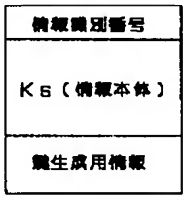
【図１】



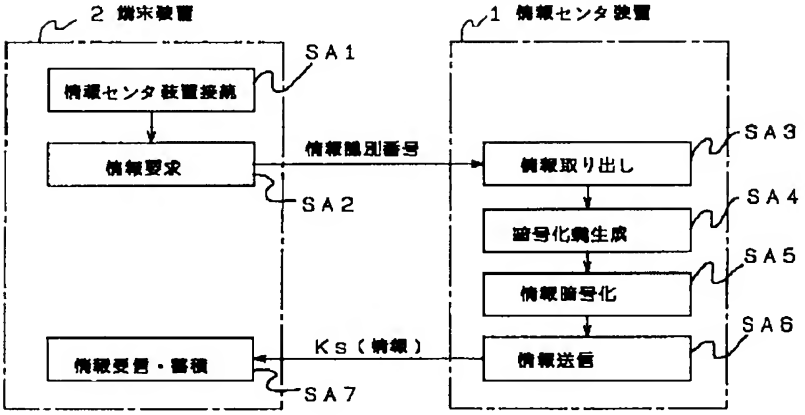
【図３】



【図７】



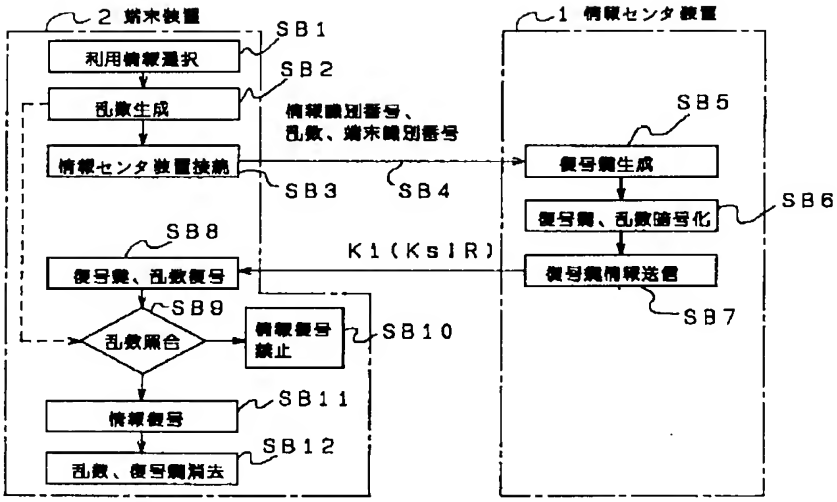
【図２】



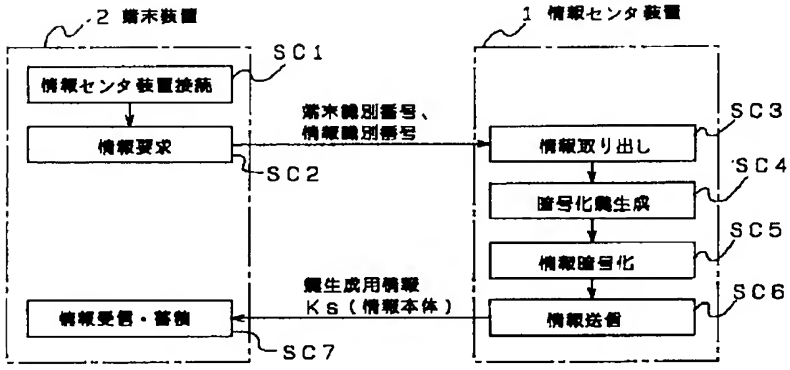
【図５】

端末識別番号	端末秘密鍵
ＩＤ１	Ｋ１
ＩＤ２	Ｋ２
ＩＤ３	Ｋ３
：	：

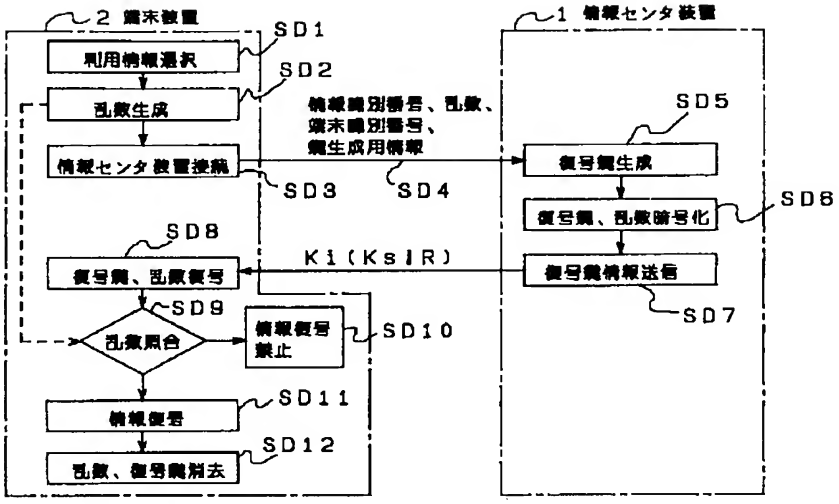
【図４】


2 端末装置
1 情報センタ装置
SB1
利用情報選択
SB2
乱数生成
情報識別番号、
乱数、端末識別番号
情報センタ装置接続
SB3
SB4
SB5
復号鍵生成
SB6
復号鍵、乱数暗号化
K1(KsIR)
SB8
復号鍵、乱数復号
復号鍵情報送信
SB7
SB9
乱数照合
情報復号
禁止
SB10
情報復号
SB11
乱数、復号鍵消去
SB12

【図６】


2 端末装置
1 情報センタ装置
SC1
情報センタ装置接続
端末識別番号、
情報識別番号
情報要求
SC2
SC3
情報取り出し
SC4
暗号化鍵生成
SC5
情報暗号化
SC6
鍵生成用情報
Ks(情報本体)
情報送信
情報受信・蓄積
SC7

【図８】



フロントページの続き

(72)発明者　神田　雅透
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　松田　伸広
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(72)発明者　関谷　邦彦
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(72)発明者　矢幡　明樹
東京都日野市旭が丘３丁目１番地の１　株式会社東芝日野工場内